1	WILLKIE FARR & GALLAGHER LLP BENEDICT Y. HUR (SBN: 224018)						
2	bhur@willkie.com						
3	SIMONA AGNOLUCCI (SBN: 246943) sagnolucci@willkie.com EDUARDO E. SANTACANA (SBN: 281668) esantacana@willkie.com ARGEMIRA FLÓREZ (SBN: 331153)						
4							
5							
6	aflorez@willkie.com HARRIS MATEEN (SBN: 335593) hmateen@willkie.com 333 Bush Street, 34 th Floor San Francisco, CA 94104						
7							
8							
9	Telephone: (415) 858-7400						
10	Attorneys for Defendant GOOGLE LLC						
11							
12	UNITED STATES DISTRICT COURT						
13	NORTHERN DISTRICT OF CALIFORNIA						
14							
15	ANIBAL RODRIGUEZ, et al. individually and on behalf of all others similarly situated,	Case No. 3:20-CV-04688 RS					
16	Plaintiff,	DECLARATION OF DAVID MONSEES ISO OMNIBUS MOTION TO SEAL DKT 473, 478, 485					
17							
18	VS.	, ,					
19	GOOGLE LLC, et al.,	Date: Time:	May 15, 2025 1:30 p.m.				
20	Defendant.	Ctrm: Judge:	3 - 17th Floor				
21			Hon. Richard Seeborg				
22		Action filed: Trial Date:	July 14, 2020 August 18, 2025				
23			S ,				
24							
25							
26							
27							
28							

- I, DAVID MONSEES, respectfully submit this declaration in regard to the above captioned matter. I make this declaration based on my personal knowledge of the facts stated herein.
- 1. I am a Senior Product Manager at Google LLC with supervisory authority concerning Web & App Activity ("WAA"). I joined Google in 2009 and have been a Product Manager since December 2009. In my role as a Product Manager at Google, I have managed various products across the advertising and WAA product areas. I am familiar with Google's practices regarding the treatment of sensitive business and technical information described herein.
- 2. Unless otherwise stated, the facts I set forth in this declaration are based on my personal knowledge or knowledge I obtained through my review of corporate records or other investigations conducted by myself or Google employees under my supervision. If called to testify as a witness, I could and would testify competently to such facts under oath.
- 3. I submit this declaration in support of Google LLC's Statement in Support of an Omnibus Motion to Seal portions of the briefing and exhibits filed in connection with Plaintiffs' Motion to Exclude Certain Opinions and Testimony of Google's Experts (Dkt. 473), Google's Opposition thereto (Dkt. 488), Plaintiffs' Opposition to Google's Motion to Exclude Sundar Pichai from Testifying at Trial (Dkt. 479), and Google's Reply thereto (Dkt. 487).
- 4. Google seeks to seal narrowly tailored portions of the aforementioned documents and exhibits. Specifically, where sensitive information is pervasive and inextricably intertwined such that redaction is infeasible, Google seeks sealing of the entire document as the narrowest possible means to protect its compelling interests. Otherwise, Google seeks to seal only select excerpts from the documents.

122950706.3

Plaintiffs' Motion to Exclude Certain Opinions and Testimony of Google's Experts (Dkt. 473)		
Documents	Portions Sought to be Sealed	
Pl.'s Daubert Ex.	Confidential business information (pgs. 5, 7, 165, 173,); Project code	
6	name U**; Project code name Al**`	

Google's Opposition to Plaintiffs' Motion to Exclude Certain Opinions and Testimony of Google's Experts (Dkt. 488)	
Documents	Portions Sought to be Sealed
	Non-public email addresses of Google employees
Opp. Ex. B	

Plaintiffs' Opposition to Google's Motion to Exclude Sundar Pichai from Testifying at Trial (Dkt. 479)				
Documents	Portions Sought to be Sealed			
Ex. 1	Non-public email addresses of Google employees; Project code name Su***			
Ex. 2	Entirety			
Ex. 3	Non-public email addresses of Google employees; Project code name Su***			
Ex. 4	Entirety			
Ex. 8	Confidential business information (-951, -987)			
Ex. 9	Non-public email addresses of Google employees, confidential business information (-981, -982)			
Ex. 10	Entirety			
Ex. 11	Non-public email addresses of Google employees; Confidential business information (-904 to -912)			
Ex. 12	Confidential business information (-763 to -766)			
Ex. 13	Non-public email addresses of Google employees			
Ex. 14	Non-public email addresses of Google employees			
Ex. 15	Non-public email addresses of Google employees			
Ex. 16	Non-public email addresses of Google employees			
Ex. 17	Non-public email addresses of Google employees			

Plaintiffs' Opposition to Google's Motion to Exclude Sundar Pichai from Testifying at Trial (Dkt. 479)		
Ex. 18	Non-public email addresses of Google employees	
Ex. 19	Entirety	
Ex. 20	Confidential business information (portions of -151 and -152)	
Ex. 22	Non-public email addresses of Google employees	
Ex. 26	Non-public email addresses of Google employees; Internal URLs	
Ex. 27	Entirety	
Ex. 28	Confidential business and technical information (portions of -531, -532)	
Ex. 29	Confidential business and technical information (-126, -136 through - 143)	
Ex. 30	Non-public email addresses of Google employees; Internal URLs	
Ex. 31	Non-public email addresses of Google employees; Internal URLs	
Ex. 32	Non-public email addresses of Google employees; Confidential business information (-845)	
Ex. 33	Entirety	
Ex. 34	Confidential business information (-484)	
Ex. 35	Entirety	
Ex. 36	Entirety	
Ex. 37	Entirety	
Ex. 39	Non-public email addresses of Google employees	
Ex. 44	Non-public email addresses of Google employees	

Google's Reply in Support of its Motion to Exclude Sundar Pichai (Dkt. 487)				
Documents	Portions Sought to be Sealed			
Reply	Project code name Su*** (3:2-4)			
Reply Appendix A	Project code name Su*** (1:3)			

4

5

7 8

9

1112

13 14

15

1617

18

1920

21

22

2324

25

26

I. Commercially Sensitive Proprietary Business and Technical Information

- 5. Daubert Exhibit 6 is the deposition transcript of Google's expert Christopher R. Knittel, Ph.D. Google seeks narrowly tailored redactions of internal project code names (U**, Al**) where they appear. These code names are confidential identifiers for non-public projects. Public disclosure presents security risks, as malicious actors could use these names to more easily identify and target specific Google projects or systems for unauthorized access or disruption. Revealing internal naming conventions can aid efforts to probe Google's infrastructure. Google carefully maintains the confidentiality of this information. The redactions are narrowly tailored, leaving only the first or second letter visible, protecting Google's confidential information while preserving the context of the testimony
- 6. Exhibit 2 (Dkt. 479-2, GOOG-RDGZ-00035752) consists of internal meeting notes from engineering and product teams concerning changes and updates to a number of user accountlevel controls. I was a participant from the product team within these meetings. Google seeks to seal this exhibit in its entirety as it pervasively contains highly sensitive commercial, technical, and internal information. The notes detail ongoing updates and progress from the team on specific feature rollouts, technical challenges encountered (e.g., in data scaling or latency), confidential deliberations on product strategy for these controls, and specific details about Google's internal systems, including data storage architecture, server configurations, specific internal code libraries underpinning key functionalities, and discussions of specific algorithmic approaches. Disclosure would provide competitors invaluable insight into Google's development lifecycle and technical solutions they could attempt to replicate, undermining Google's competitive position built on proprietary engineering. Furthermore, revealing specifics about internal systems and technical identifiers could provide a roadmap for malicious actors seeking to exploit potential vulnerabilities in specific infrastructure components. Because this sensitive strategic, technical, and operational information is deeply interwoven, redaction would destroy necessary context. Full sealing is the narrowest means possible.

- 7. **Exhibit 4** (Dkt. 479-4, GOOG-RDGZ-00018661) is an internal Google Product Requirements Document ("PRD"). PRDs like this are foundational strategic documents at Google, outlining confidential proposals for new or updated features, reflecting significant investment in research and planning. This PRD contains non-public, competitively sensitive information including Google's internal analyses, strategic planning, specific metrics targets, product improvement goals, technical approaches, and proprietary research. Disclosure would reveal Google's confidential product strategy and roadmap. Competitors could exploit this information to anticipate Google's market moves, potentially preempting feature launches, adjust their own product strategies to directly counter Google's planned direction, replicate Google's features without incurring similar R&D costs, and otherwise undermine Google's competitive position. Given that the document's core purpose is to lay out this interwoven strategic and technical plan, redaction is infeasible. Sealing the entire exhibit is necessary.
- 8. **Exhibit 8** (Dkt. 479-8, GOOG-RDGZ-00056947) is an internal Google presentation regarding Google's Firebase platform. Google seeks narrow redactions of a specific chart on page -951 displaying sensitive internal analysis concerning the specific business impact and competitive positioning of Google's Firebase services relative to named competitors. The chart contains commercially sensitive analysis; disclosure would provide competitors valuable insights into Google's confidential assessment of the market and its performance against specific rivals, which they could use to refine their strategies.
- 9. **Exhibit 9** (Dkt. 478-9, GOOG-RDGZ-00076980) is an internal document on Firebase history. Google seeks narrow redactions of: (1) non-public employee email addresses; and (2) specific Objectives and Key Results ("OKRs") on pages -981 and -982. OKRs represent confidential internal strategic priorities and quantifiable goals, such as specific targeted growth rates, feature launch timelines, and internal efficiency goals for the Firebase organization. Disclosing these specific Firebase OKRs would reveal highly sensitive information about its strategic focus and internal performance benchmark. This is information competitors could exploit

to understand Google's strategic priorities, anticipate specific feature launches, or gain an unfair advantage.

- 10. **Exhibit 10** (Dkt. 479-10, GOOG-RDGZ-00163898) is an employee "perf packet," prepared by a Google product manager for a performance review. Google seeks to seal this document in its entirety due to the pervasive and interwoven nature of multiple categories of highly sensitive information. This performance review document compiles: (a) confidential, proprietary technical details about product functions, data storage systems, and trade secrets; (b) highly confidential and personal employee performance information (self-assessment, reviews, level, goals), disclosure of which would impede on the employees' privacy and potentially cause professional harm; and (c) discussions of numerous internal projects and related strategic projections. Public disclosure risks competitive harm, security vulnerabilities, and infringes on employee privacy. Because this sensitive technical, strategic, personnel, and internal naming information is inextricably linked throughout the "perf packet," redaction is infeasible.
- 11. **Exhibit 11** (Dkt. 479-11, GOOG-RDGZ-00057867) is an internal Google Analytics for Firebase presentation. Google seeks to seal only slides -885 through -915, which contain internal brainstorming described as "design concepts" and "what-if" scenarios for potential future product development. This represents confidential and competitively sensitive future-looking business strategy. Public disclosure would provide competitors with valuable, unearned insights into Google's potential product evolution and strategic thinking, allowing them to potentially preempt or counter Google's moves. The request is narrowly tailored to these specific forward-looking concept slides.
- 12. **Exhibit 12** (Dkt. 479-12, GOOG-RDGZ-00060716) is an internal presentation on Firebase user engagement. Google seeks narrow redactions of: (1) a non-public employee email address; and (2) slides -763 through -766 containing confidential case studies identifying specific third-party customers and detailing their performance data using Google services. Public disclosure would reveal sensitive details about the effectiveness of Google's services, confidential information about Google's customers and the results their businesses obtained via Google's

Case 3:20-cv-04688-RS

5

8

9

11

1213

1415

1617

18

20

21

19

2223

2425

26 27 products, and implicate confidential customer relationships. Competitors could use this information to target Google's customers or benchmark against Google's performance.

- 13. Exhibit 19 (Dkt. 479-19, GOOG-RDGZ-00130078) consists of extensive internal meeting notes detailing deliberations among the leadership of Google's Geo organization (responsible for products like Maps, Earth, Street View) spanning approximately eight months in 2018. Google seeks to seal this exhibit in its entirety due to the pervasive nature of highly sensitive strategic, commercial, and operational information integral to Google's competitive positioning. These notes contain: specific product roadmaps and launch timelines (including for Discovery, Commute features, Universal Local Campaigns, games, and Google Maps Platform); confidential key performance indicators and internal goals (like specific DAU figures for GMB and Assistant, iOS penetration rates versus competitors, revenue figures and targets, NPS data, and feature adoption percentages); internal assessments critiquing product performance and partner feedback; and sensitive competitive intelligence and market analysis. Public disclosure of these detailed, high-level strategic notes, metrics, and internal assessments would cause significant competitive harm by revealing Google Geo's long-term strategy, confidential internal performance data, product pipeline secrets, operational challenges, competitive vulnerabilities, and sensitive partnership information, allowing competitors to unfairly benchmark against Google and counter its strategies. Because this comprehensive strategic, financial, competitive, and operational information is deeply interconnected and woven throughout the notes covering months of leadership discussions, redaction of isolated pieces of information would be impracticable and fail to protect the vast amount of confidential strategic information presented. Full sealing is therefore the narrowest means necessary.
- 14. **Exhibit 20** (Dkt. 479-20, GOOG-RDGZ-00127151) is an email summarizing an internal "Google Leads" meeting. Google seeks narrow redactions of specific excerpts on pages 151 and -152 containing highly sensitive, non-public information unrelated to the points Plaintiffs cite (Brief §§ III.A.1, III.A.2). These redactions cover: (a) internal deliberations regarding managing internal communications and potential leaks, disclosure of which presents operational

risks; (b) confidential commercial information including negotiation strategies and status updates regarding key partners/competitors, disclosure of which could severely compromise Google's negotiating position; and (c) internal strategic assessments relative to competitors. These redactions are narrowly tailored to protect these deliberations.

- document assessing a proposal regarding retention of WAA-On Data. Google seeks to seal this document entirely due to pervasive, highly sensitive technical, strategic, and financial information. It contains detailed discussions of internal servers, data logging specifics, internal logging "TTLs" (short for time-to-live periods), non-public metrics including rates of Daily Active Users across various features, modeling and analyses of costs and revenue impact, discussions of efforts sensitive fraud and spam detection measures, plans for changes to future systems, and internal hyperlinks and non-public email addresses. Disclosure would expose proprietary technical systems, data handling processes, internal metrics, financial models, and strategic deliberations, causing significant competitive harm by granting Google's competitors unearned insight into Google's product strategy. It could also provide a detailed roadmap for malicious actors seeking to understand and potentially compromise Google's systems. The sensitive information is deeply integrated throughout the document, making redaction infeasible .
- 16. **Exhibit 28** (Dkt. 478-28, GOOG-RDGZ-00061531) is an internal FAQ on WAA default retention changes. Google seeks narrow redactions of: (1) non-public employee email addresses; (2) a specific internal projection on page -531 regarding the number of users subject to a proposed setting change; (3) specific technical details on page -532 regarding internal data deletion policies, affected internal logs, technical mechanisms for downstream systems, and internal URLs; and (4) related comments discussing this sensitive information. This exhibit exposes highly technical and downstream systems for managing data retention and deletion requests. Disclosing its contents could provide competitors with unearned insight into Google's data retention architecture and potentially allow bad actors to exploit portions of this architecture.

- 17. **Exhibit 29** (Dkt. 478-29, GOOG-RDGZ-00046121) is an internal strategy document for changes to the WAA, YouTube History, and Location History default retention settings. Google seeks narrow redactions covering multiple categories of sensitive information.

 Specifically, Google seeks to redact sensitive technical implementation details on page -126 and pages -136 through the end. The proposed redactions cover information providing the specifics of technical pipelines, downstream systems, internal system names/identifiers, and bug tracking details; discussion of legal review; and, insights from confidential user research studies. Google also seeks to redact non-public employee email addresses and internal URLs. Disclosure of the information contained in this document would provide competitors with valuable insight into the structure of Google's data processing systems, which could give them an unearned windfall.

 Additionally, the information Google seeks to redact can be used by bad actors to attempt to gain access to Google's systems.
- 18. **Exhibit 32** (Dkt. 479-32, GOOG-RDGZ-00127840) is an internal email. Google seeks narrow redactions of: (1) non-public employee email addresses; (2) a specific, non-public internal statistic on page -845 regarding user interaction metrics. This internal performance metric is confidential; disclosure would reveal non-public data about the usage of Google's account features potentially allowing competitors to benchmark against Google.
- 19. **Exhibit 33** (Dkt. 478-33, GOOG-RDGZ-00188868) is an internal Google document prepared by Google's Privacy and Data Protection Office, marked internally with access restrictions ("need to know," "do not forward"). Google seeks to seal this document in its entirety. This document reflects a significant internal fact-gathering and analysis project undertaken by Google in advance of considering various proposed product changes. It compiles information gathered through confidential interviews with numerous Google employees involved with a wide variety of Google products and services, including but not limited to Google Docs, Gmail, and Google Maps. The core purpose of this extensive effort, which required substantial investment of Google's time and internal resources, was to conduct internal user and product research to gather candid perspectives and data points. This research directly informs Google's confidential product

roadmap development, strategic planning, and critical decisions regarding potential future features or modifications across these key product lines. This type of internal strategic analysis and research constitutes highly sensitive proprietary business information. Public disclosure of this document would inflict significant competitive harm by providing competitors with an unearned windfall *i.e.* direct access to the insights gleaned from Google's resource-intensive internal research effort. Competitors could exploit these detailed findings about internal perspectives, potential user needs, and cross-product considerations to unfairly accelerate their own product development, refine their strategies to directly counter Google's potential direction, and gain market advantages without investing the considerable effort and expense Google undertook.

Because the document's value lies precisely in this comprehensive compilation of internal research findings spanning multiple products, redaction of specific portions is infeasible without revealing the very insights Google invested heavily in gathering and seeks to protect. Therefore, sealing the entire exhibit is necessary and narrowly tailored to safeguard Google's interests.

- 20. **Exhibit 34** (Dkt. 478-34, GOOG-RDGZ-00203483) is an internal marketing leadership update email. Google seeks narrow redactions of (1) confidential internal statistics on page -484 regarding Daily Active Users (DAUs) and specific platform traffic data following a Super Bowl ad campaign; and (2) non-public employee email addresses. The data Google seeks to redact constitutes proprietary internal metrics, disclosure of which would reveal confidential user engagement levels and Google's internal measurement of its marketing efforts. These are insights competitors could leverage to benchmark their own ROI or to refine marketing strategies against Google.
- 21. **Exhibit 35** (Dkt. 479-35, GOOG-RDGZ-00039515) is an internal email thread discussing a non-public technical proposal for logging location information. Google seeks to seal this exhibit in full due to its sensitive technical nature. It details proprietary methods regarding how and where certain data is logged within Google's internal systems and infrastructure. Public disclosure would reveal specific internal data handling processes, which would be valuable to

8

9

11

1415

1617

18

1920

2122

23

2425

26

27

28

competitors attempting to reverse-engineer Google's systems and potentially provide a roadmap for malicious actors seeking to understand or compromise these systems.

- 22. Exhibit 36 (Dkt. 479-36, GOOG-RDGZ-00153597) consists of internal notes documenting recurring one-on-one ("1:1") sync meetings between two senior engineers within Google's Geo organization, spanning nearly three years. Google seeks to seal this document in its entirety due to the pervasive and intertwined nature of highly sensitive technical and confidential personnel information discussed within these private syncs. The notes capture two main categories of information arising naturally from these engineers' collaborative work and management responsibilities: (1) Detailed, proprietary technical engineering discussions concerning their ongoing work, including challenges, progress, architectural decisions, and specific operational details related to Google's internal systems for location services, the disclosure of which risks competitive and security harm by revealing trade secrets and potentially exploitable system information; and (2) Highly confidential personnel and team management matters, including internal assessments of team staffing needs, hiring strategy discussions, sensitive feedback and specifics regarding individual team members (including related to performance, promotions, and re-organizations), and evaluations of potential job candidates, the disclosure of which would infringe employee privacy expectations and reveal confidential internal HR deliberations. Because these technical work discussions and sensitive personnel matters are naturally and inextricably intertwined within the context of these confidential 1:1 meetings between senior colleagues responsible for both technical execution and team oversight, redaction is infeasible.
- 23. **Exhibit 37** (Dkt. 479-37, GOOG-RDGZ-00017489) consists of internal notes from recurring one-on-one ("1:1") sync meetings between two different engineers within Google's Geo organization, documenting their collaborative engineering work. The notes predominantly contain detailed, proprietary technical and engineering discussions regarding the specific internal systems and infrastructure these engineers were developing or maintaining, particularly concerning the internal logging of location information. This includes specifics about system design, implementation choices, technical challenges encountered, and operational details which

 constitute Google trade secrets and confidential technical information. Public disclosure of this sensitive technical substance would provide competitors with valuable insights into Google's proprietary internal methods and operational details, and could pose security risks if specific system architecture or logging mechanisms were revealed and potentially exploited by malicious actors. Given that the document's primary focus is this pervasive, sensitive technical discussion relating to their engineering tasks, redaction is infeasible without revealing the core proprietary engineering details Google seeks to protect.

- 24. **Non-Public Email Addresses.** Certain exhibits, as listed below and noted in Google's [Proposed] Order, contain non-public. Google does not publicly publish its internal employee email address formats or specific addresses. Allowing these internal email addresses to become public presents a threat of harassment, phishing, or unwanted contact directed at these employees, many of whom are not parties to this action. Protecting this information serves the privacy interests of these individuals. Google has narrowly tailored the requested redactions to seal only the unique identifier portion of the email address (e.g., redacting only [uniqueaddress] in an address like "First Name Last Name <[uniqueaddress]@google.com>"), leaving the employee's name and the Google domain visible. No more limited sealing would adequately protect these individuals' privacy interests. I understand this Court has previously permitted such redactions. See, e.g., Dkt. 284; Dkt. 353. Google seeks redaction of non-public employee email addresses in the following exhibits: *Daubert* Opposition Ex. B, Pichai Opp. Exhibits 1, 3, 8, 9, 11, 12, 13, 15, 16, 17, 18, 20, 22, 26, 28, 29, 30, 31, 32, 34, 39, 44.
- 25. **Internal Codenames and URLs.** Certain exhibits, as listed below and noted in the table, reference internal project codenames, internal URLs pointing to non-public internal Google pages (such as documents, tools, code repositories), and/or internal names for portions of Google's technical architecture (such as servers, data logs, and databases). This information is confidential and used internally for project management and technical operations.
- 26. Public disclosure presents security risks. Malicious actors could use codenames or technical identifiers to more easily target specific Google projects, systems, or data for

unauthorized access, disruption, or theft. Knowledge of internal naming conventions, system
identifiers, or internal structures revealed by URLs can aid efforts to probe or compromise
Google's infrastructure, and potentially provide vectors for social engineering or targeted attacks.
Disclosure also harms competitive interests by potentially revealing the focus, nature, or technical
underpinnings of non-public projects or systems. Google implements measures to keep this
information confidential.

27. Google seeks narrowly tailored redactions, typically redacting most letters of a codename, the entirety of internal URLs, or specific server/log/schema/tool names where they appear. This obscures the sensitive identifier while generally leaving surrounding context intact. I understand this Court has previously recognized the sensitivity of such identifiers and permitted their sealing (e.g., Dkt. 284; Dkt. 353). Google seeks to redact internal codenames, URLs, or internal technical names in: Plaintiffs *Daubert* Ex. 6; Google's Pichai Reply; Google's Pichai Reply Appendix A; Exhibits 1, 3, 8, 12, 28, 29, 30, 31.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed May 1, 2025, at San Francisco, California.

David Monsees